

Amendments to the Claims:

The following listing of the claims replaces all previous listings and versions of the claims in the application:

Listing of the Claims:

Claims 1-19: (Cancelled)

20. (Currently Amended) A method of establishing a communication path ~~from a first identity device having an identity representing a first legal entity in a data communication network~~ from a chip card associated with a client, comprising the steps of:

providing a ~~one-time-only~~ privacy reference point in said data communication network, said privacy reference point configured for use in one transaction;

establishing a first communication path ~~from the first identity device~~ said chip card to said ~~one-time-only~~ privacy reference point;

providing an authentication of ~~the first identity device~~ said chip card relative to said ~~one-time-only~~ privacy reference point;

verifying the authentication of ~~the first identity device~~ said chip card relative to said ~~one-time-only~~ privacy reference point from said ~~first identity device~~ chip card; and

establishing a second communication path ~~from a first communication device associated with a first entity to said one-time-only privacy reference point to a second identity device representing a second legal entity~~ through said data communication network;

wherein at least one of the steps of verifying the authentication and establishing a second communication path is performed without disclosing the identity of said ~~first identity device~~ chip card.

21. (Currently Amended) The method according to claim 20, wherein the step of providing an authentication comprises the steps of:

~~authenticating said first identity device by~~ registering data selected from the group consisting of biometrics, a signature, a code, and any combinations thereof; and

comparing the registered data with ~~correspondingly~~ corresponding stored data.

22. (Currently Amended) The method of claim 20, wherein the step of verifying the authentication is performed without disclosing the identity of ~~the first identity device~~ said chip card.

23. (Currently Amended) The method of claim 20, wherein the step of establishing a second communication path is performed without disclosing the identity of ~~the first identity device~~ said chip card.

24. (Currently Amended) The method according to either of claims 20 or 21, wherein ~~said first identity device comprises a chip card including~~ includes encrypted data, said method further comprising:

said ~~first identity device~~ chip card receiving an encrypted key from said ~~one-time-only~~ privacy reference point;

decrypting said encrypted key using a second stored key to create a decrypted version of the encrypted key; and

decrypting said encrypted data using the decrypted version of said encrypted key.

25. (Previously Presented) The method according to either of claims 20 or 21, said communication network being selected from a group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

26. (Currently Amended) The method according to either of claims 20 or 21, ~~said first identity device~~ chip card having an authenticated holder, and said ~~one-time-only~~ privacy reference point

being addressable by the authenticated holder from a computer communicating with said data communication network.

27. (Currently Amended) The method according to either of claims 20 or 21, further comprising said ~~first identity device~~ chip card allowing or blocking access to said ~~one-time-only~~ privacy reference point by a ~~third identity~~ second communication device.

28. (Cancelled)

29. (Currently Amended) The method according to either of claims 20 or 21, wherein at least one of said steps of establishing a first communication path and establishing a second communication path involves creating and negotiating an accountability path adapted to a context risk profile.

30. (Currently Amended) The method according to claim 29, wherein said ~~first identity device~~ chip card has an authenticated holder, and said ~~second identity device~~ first communication device establishes a procedure to identify a party selected from a group consisting of said ~~first identity device~~ chip card and the authenticated holder of said ~~first identity device~~ chip card.

31. (Previously Presented) The method according to claim 30, wherein said procedure to identify a party employs identification information selected from a group consisting of at least one of biometrics, name, digital signature, and a code.

32. (Currently Amended) The method according to either of claims 20 or 21, further comprising:  
    providing an identity provider and a service provider;  
    establishing communication from said ~~second identity~~ first communication device to said service provider;  
    establishing communication from said service provider to said identity provider;

providing a further ~~identity communication~~ device ~~corresponding to~~ associated with a financial institution;

establishing communication from said service provider to said further ~~identity communication~~ device;

transmitting information from said ~~second identity~~ first communication device to said service provider;

transmitting said information from said service provider to said identity provider;

transmitting said information from said identity provider to said further ~~identity communication~~ device;

said further ~~identity communication~~ device responding to said information by transmitting a payment acceptance to said identity provider;

said identity provider transmitting said payment acceptance to said service provider; and

said service provider transmitting said payment acceptance to said ~~second identity~~ first communication device.

33. (Currently Amended) A system for establishing a communication path in a data communication network from a ~~first identity device chip card~~ having an identity ~~representing a first legal entity associated with a client~~ in a data communication network, comprising:

a ~~one-time-only~~ privacy reference point in said data communication network, said privacy reference point configured for use in one transaction; and

a first communication path ~~defined from said first identity device chip card~~ to said ~~one-time-only~~ privacy reference point;

~~means for providing an authentication of the first identity device relative to said one-time-only privacy reference point~~;

means for verifying ~~the~~ an authentication of said ~~first identity device chip card~~ relative to said ~~one-time-only~~ privacy reference point from said ~~first identity device chip card~~; and

~~means for establishing a second path of communication path~~ from said ~~one-time-only~~ privacy reference point to a ~~second identity communication~~ device representing a ~~second legal~~ an entity through said data communication network;

wherein at least one of the means for verifying the authentication and the ~~means for establishing second~~ communication path is operable without disclosing the identity of said ~~first identity device chip card~~ to said ~~second identity communication~~ device.

34. (Currently Amended) The system according to claim 33, wherein said ~~one-time-only~~ privacy reference point is stored on a server communicating with said data communication network.

35. (Previously Presented) The system according to either of claims 33 or 34, wherein said data communication network is selected from a group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

36. (Currently Amended) The system according to either of claims 33 or 34, wherein said ~~first identity device comprises a chip card including~~ includes encrypted data for verifying the authentication of the ~~first identity device chip card~~ relative to said ~~one-time-only~~ privacy reference point.

37. (Previously Presented) The system according to either of claims 33 or 34, wherein said means for verifying employs data selected from a group consisting of at least one of biometrics, and codes, and digital signatures.

38. (Currently Amended) The system according to either of claims 33 or 34, wherein said means for verifying the authentication is operable without disclosing the identity of said ~~first identity device chip card~~ to said ~~second identity communication~~ device.

App. No.: 10/575,416  
Amendment to Office Action of June 18, 2009  
Docket No.: 606-128-PCT-PA

39. (Currently Amended) The system according to either of claims 33 or 34, wherein said ~~means~~  
~~for establishing~~ second communication path is operable without disclosing the identity of said  
~~first identity device chip card~~ to said ~~second identity communication~~ device.